iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XI **Month of publication:** November 2021

DOI: https://doi.org/10.22214/ijraset.2021.38985

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

A Comprehensive Analysis and Recommendations on Network Monitoring Tools

Mohammad Shariful Islam
Post Graduate Student, Dept. of EE & CE Military Institute of Science and Technology, Mirpur Cantonment, Dhaka, Bangladesh

Abstract: ***A high-performance network is a necessary component of any company's IT infrastructure. All operations, including internal and external communication across different corporate sites, as well as communication with clients and partners, should operate smoothly to enable smooth business activities. Failures and malfunctions in operational procedures can easily result in lost time and money. In order to maintain track of the availability, performance, and bandwidth utilization in an IT network, network monitoring software that continuously monitors operations in the network, does analysis, and warns IT workers as soon as an error happens or critical values are surpassed is highly recommended. If the administrator is not on site, network monitoring allows him or her to intervene swiftly, even if he or she is not there. Of course, each firm has unique requirements for a network monitoring solution, and with so many tools and solutions on the market, careful selection of an appropriate solution is essential. This paper discusses the different alternatives that a network solution can provide provided the appropriate criteria are taken into account during the decision-making process.***
Keywords: Network, Network Monitoring Tools, IT infrastructure, Open Source

I. INTRODUCTION

The purpose of this paper is to make a recommendation for choosing the best network monitoring tools for a company by examining and comparing their strengths and weaknesses. Network monitoring is an important aspect of defending any company's infrastructure in today's world of ongoing security threats. After all, the correct network monitoring system may increase uptime and efficiency while also alerting you to potential security breaches before they create costly outages. A robust network monitoring software may save busy IT workers many hours of monitoring switches, routers, servers, and other devices. Network monitoring software can minimize the need to sit in front of a screen for hours at a time, providing you the assurance that no matter where you are, you will be warned of any problems before they become serious. By examining and comparing their strengths and weaknesses, the goal of this paper is to provide a suggestion for picking the best network monitoring tools for a company.

II. BACKGROUND

Keeping the network up, running, and supporting business services is more than critical for all firms - it's the enabler of daily operations, from employee productivity to customer service. Employees and customers need to be able to access services, as well as efficiency and overall quality. This is especially true in today's remote work environment, which has been exacerbated by the COVID-19 pandemic. As a result, every firm requires tools that offer network status and maintain service availability while assuring adequate capacity. It's also crucial to note that in many firms, an IT group is responsible for practically every aspect of technology, including hardware, installation, setup, application implementation, and security. Furthermore, data centres, collocated environments, and the cloud are all typical locations for technology assets. As a result, IT has become more complex, necessitating a more unified perspective of network operations. Businesses are exposed to a wide range of dangers and vulnerabilities if they don't have reliable network monitoring software. However, the truth is that risks can sometimes turn into network events, and network events might turn into outages. IT is still working with faulty systems, even with the most advanced technologies and built-in redundancy. Downtime is frequently caused by seemingly minor errors:

1) Lack of network documentation
2) Limited information on network configurations
3) Ineffective means for identifying and tracking devices on the network
4) Inability to identify ISP connections
5) Lack of visibility into performance
6) Inability to identify root causes

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XI Nov 2021- Available at www.ijraset.com

In today's digitally driven world, the most serious consequence of downtime is the inability to recover as a company, albeit the reasons for this can vary. Because IT services were down, a firm may have lost personnel due to the inability to pay employees on schedule. Or perhaps the service provided was not supplied on time due to insufficiently available or performant systems. Other repercussions include, but are not limited to, lost productivity, revenue, and non-quantifiable expenses such as abandoned IT efforts, harmed IT morale, and missed market opportunities (Mission Critical Magazine). To make informed decisions, every organization requires network visibility and actionable intelligence. Consequential safeguards against downtime include resource planning, performance improvements, and security measures. For example, if a corporation wants to add additional resources, such as a new productivity application, predicting how much bandwidth the application will require is exceedingly difficult. In today's fast-paced, customer-centric business climate, such a lag can significantly hinder an organization's ability to expand and adapt. However, with the right network monitoring system, it becomes possible to effectively monitor status, resources, and performance for applications and services. In essence, IT is constructed on top of the network; everything needs to be connected to the internet to work. There's no way to link the network to everything it's connected to without network visibility, performance control, or analytics.

A. Problem Statement

According to a recent estimate, in 2021, any networks, remote working software, and cloud systems will be the target of a new wave of attacks. In 2021, cybercriminals will use residential networks as a critical launching pad for attacking corporate IT and IoT networks. You must consider a number of aspects when choosing a network monitoring solution for your company. While understanding the advantages of network monitoring is pretty simple, selecting the proper software can be a challenge. Network monitoring software isn't all made equal. IT and business leaders must choose the one that offers the best security for their company's sensitive data. Because of the importance of this job, there are a few things to think about when choosing a network monitoring system.

B. Rationale of the study

Business disruptions are caused by network breakdown. When such disruptions occur, businesses lose clients, resulting in significant losses and a drop in employee productivity. Due to downtime, 33% of SMBs have lost revenue and customers. According to another studies, downtime reduces employee productivity by 21%. Network monitoring aids in the proactive resolution of network issues before they occur. Such solutions help organizations retain consumers and increase employee productivity by reducing downtime. This paper discusses the different alternatives that a network solution can provide provided the appropriate criteria are taken into account during the decision-making process.

C. Research questions

1) What is the purpose of investing in the network monitoring tool?
2) What about prize and licensing: is the solution opensource? is the solution free?

D. Research Gap

Every firm has various needs for a network monitoring solution, and with so many different tools and solutions on the market, careful selection of the right one is essential. Because one solution may not be appropriate for every firm, selecting a monitoring system is also tricky.

III. METHODOLOGY

In order to address the research questions, the following technique will be used.
Direct observation: At this stage, all of the necessary information will be gathered by observing both online and offline applications and tools.
This survey and questionnaire portion will be completed online. The survey URLs will be emailed to the IT directors of various firms and institute directors, among others.
Observing the underground community through online chats and conversations will also be a useful method of gathering information.
Not only that, but asking questions and posting questions can also be a very useful way of gathering knowledge. The preferred technique for this research paper is to incorporate all types of organizations so that they can participate. The acquired data will be analysed in a methodical and logical manner in order to test the hypothesis and determine if it is proof or disproof.

IV. RESULTS

1) Comparison for Network Monitoring Tools Table 1

Name of tools	Free trial	Platform	Business Size	Deployment	Price	Support
SolarWinds	30 days	Windows & Linux	Small to large businesses	On-Premise	Starts at per agent $60 a month	Real time 24/7 Live Chat Support
Datadog	14 days	Windows, Mac, Linux	Small to large businesses	On-premise and SaaS.	Starts at $5/host/month	Chat support business hours of 10:00 and 19:00 ET.
ManageEngine OpManager	30 days	Windows, Linux, iOS, and Android	Small to large businesses	On-premise	US$395, 1 user/ 10 Monitors	24x7 tech support over toll free number
Site24x7	30 days	Windows & Linux	Small to large businesses	Cloud	Starts at $9/month	Monday – Friday 24hrs Support
Nagios	60 days	Windows, Linux, Mac, & UNIX	Small to large businesses	Cloud & On-Premise.	$1995 for a single license.	US office hours

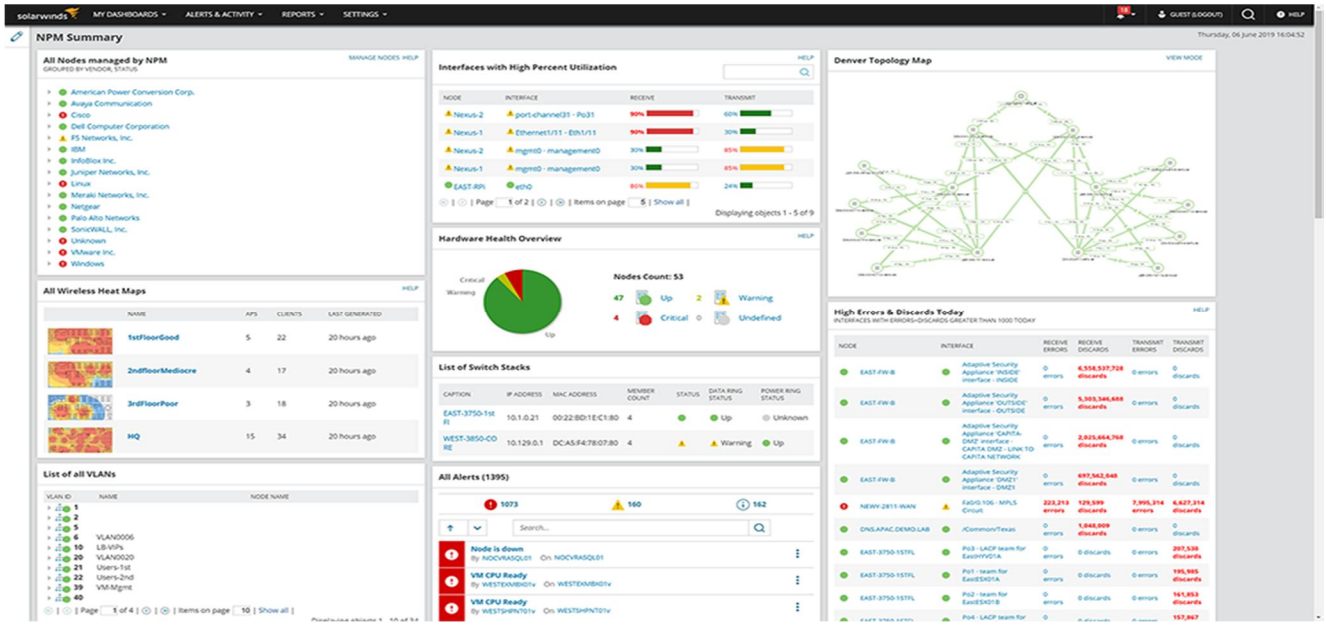
2) Comparison for Network Monitoring Tools Table 2

Name of tools	Features	Pros	Cons
SolarWinds Network Performance Monitor	Multi-vendor network monitoring Network Insights for deeper visibility Intelligent maps NetPath and PerfStack for easy troubleshooting Smarter scalability for large environments Advanced alerting	Real-time monitoring Instant up/down of network devices across all networks Top talkers in different ways (IP, application, and others) Auto-discovery is very easy for devices. inbuilt scanner from LAN network to get auto network discovery.	This is not compatible with minimal hardware and OS. Dependency on latest SQL Version license. During installation, the application crashed in many scenarios. Does not have device configuration backup option. Not all devices are supported
Datadog Network Performance Monitoring	Datadog Network Performance Monitoring (NPM) enables you to get unprecedented visibility into modern networks using meaningful, human-readable tags. It maps the flow of network traffic between hosts, containers, availability zones, and even more abstract concepts like services, teams, or any other tagged category. It correlates network traffic data with relevant application traces, host metrics, and logs, to unify troubleshooting into one platform. Visually maps traffic flow in an interactive map to help identify traffic bottlenecks and any downstream effects.	Application Monitoring Log Management Visualization Error finding Easy to implement	Agent-based. Initial learning curve Azure integration is not easy Events Tracking Infrastructure flow visualization
ManageEngine OpManager network monitoring	Real-time network monitoring Physical and virtual server monitoring Multi-level thresholds Customizable dashboards WAN Link monitoring Affordable and easy to set up	Network Monitoring Alerting, Reporting Agentless monitoring Automation Network discovery	Scalability Options Some legacy products is complicated to add. Out of the integrations with 3rd party tools Do not have a sensor for Azure or AWS metrics

Name of tools	Features	Pros	Cons
Site24x7—A complete network monitoring software	Auto-discovery Multi-vendor Support Device Templates Network Mapping Health Dashboard SNMP Trap Processing Sensor Monitoring Support for Custom MIBs VoIP Monitoring	Certificate monitoring Website monitoring Real user monitoring Good accuracy Very lightweight agent.	Interface is a little confusing. Cost Seems lit bit expensive. Setup is complicated Confusing selecting the right monitor A lot of false positives
Nagios - The Industry Standard In IT Infrastructure Monitoring	Advanced Graphs & Visualizations Performance & Capacity Planning Graphs Configuration Wizards Advanced Infrastructure Management Configuration Snapshot Archive Advanced User Management Service-Level Agreement (SLA) Reports Extendable Architecture	Monitor IT asset Reports generation Service and host metrics Easy-to-use GUI Great cost-value balance	The initial configuration is a little tricky. Native applications for Graphics Steep Learning curve Golang integration No real-time graphing unless an add-on is installed.

A. SolarWinds Network Performance Monitor

SolarWinds is a significant provider of IT management software around the world. One of the company's primary products is the Network Performance Monitor (NPM). This system is designed to keep track of the health of networked devices. Network equipment, such as routers and switches, endpoint devices, such as terminals, desktop PCs, and mobile devices, and office equipment, such as printers, are among the hardware that SolarWinds Orion NPM monitors. The continuous monitoring procedure collects parameters that help with troubleshooting.

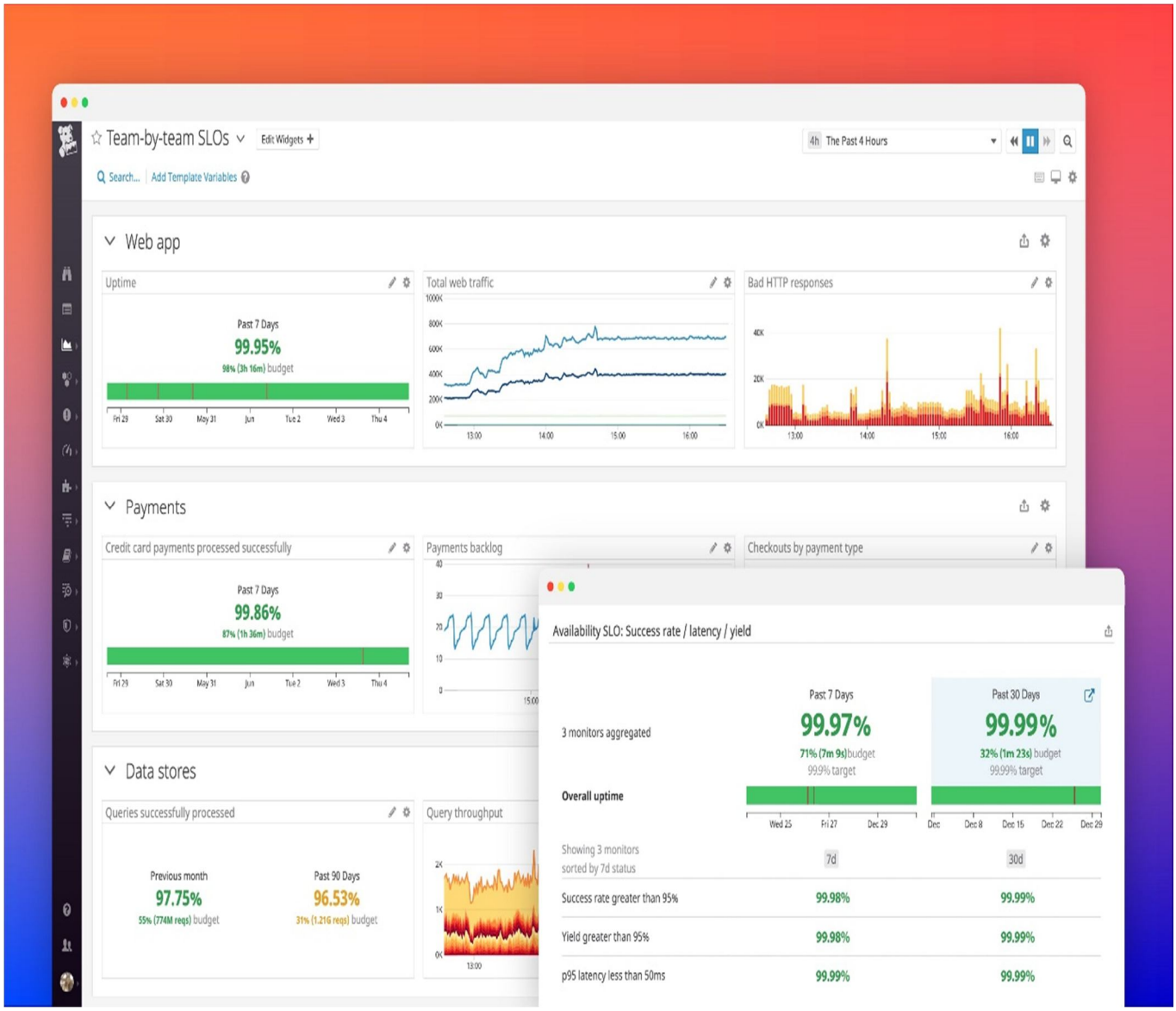


Features:

1) Multi-vendor network monitoring
2) Network Insights for deeper visibility
3) Intelligent maps
4) NetPath and PerfStack for easy troubleshooting
5) Smarter scalability for large environments
6) Advanced alerting

B. Datadog Network Performance Monitoring

Datadog Network Performance Monitoring (NPM) is a tool that shows you how much traffic is flowing between services, containers, availability zones, and any other tag in Datadog. Application-layer dependencies between meaningful source and destination endpoints are gathered from connection data at the IP, port, and PID levels, and may be studied and displayed using a configurable network page and network map. Flow data, as well as important network traffic and the DNS server, should be used.

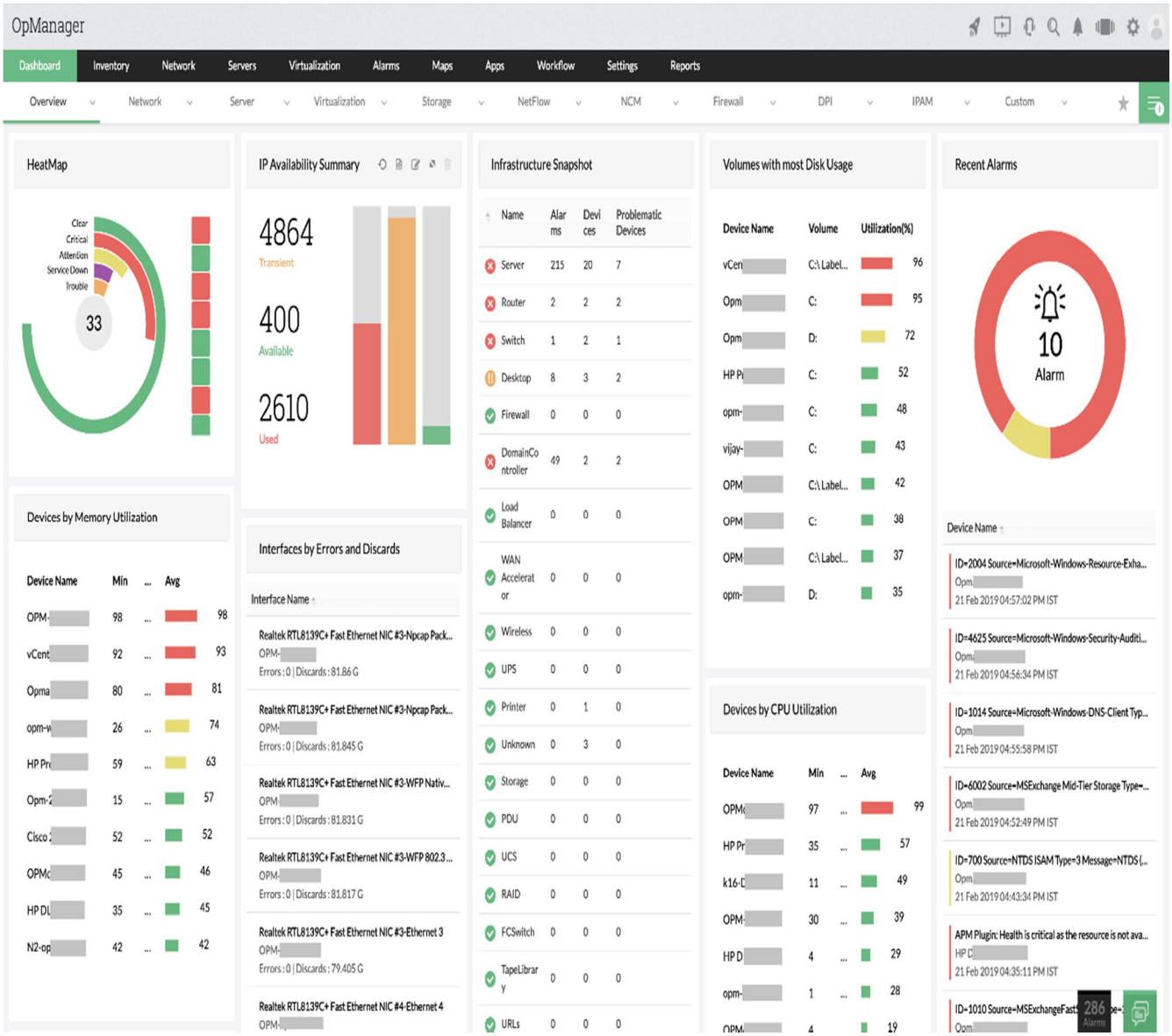


Features:

1) Datadog Network Performance Monitoring (NPM) enables you to get unprecedented visibility into modern networks using meaningful, human-readable tags.
2) It maps the flow of network traffic between hosts, containers, availability zones, and even more abstract concepts like services, teams, or any other tagged category.
3) It correlates network traffic data with relevant application traces, host metrics, and logs, to unify troubleshooting into one platform.
4) Visually maps traffic flow in an interactive map to help identify traffic bottlenecks and any downstream effects.

C. ManageEngine OpManager network monitoring:

Introducing ManageEngine OpManager is a simple and cost-effective network monitoring solution. It keeps track of routers, switches, firewalls, load balancers, wireless LAN controllers, servers, virtual machines, printers, storage devices, and everything else with an IP address and a network connection. ManageEngine OpManager keeps a constant eye on the network and gives you complete insight and control over it. You can simply dive down to the underlying source of a problem and eliminate it before operations are harmed.

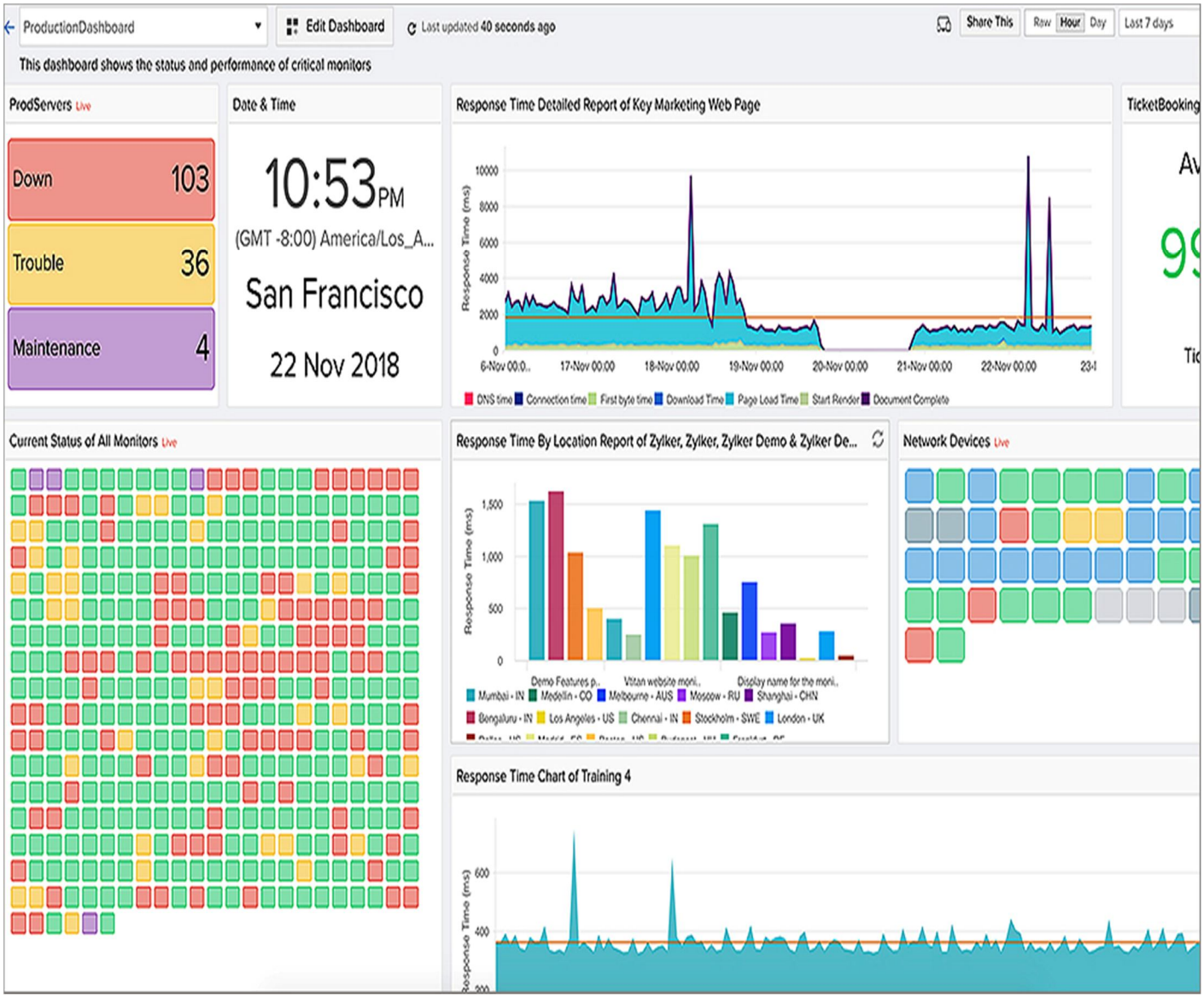


Features:

1) Real-time network monitoring
2) Physical and virtual server monitoring
3) Multi-level thresholds
4) Customizable dashboards
5) WAN Link monitoring
6) Affordable and easy to set up

D. Site24x7—A complete Network Monitoring Software

With Site24x7 comprehensive cloud network monitoring tool, one you can easily drill down to the root cause of network issues with the in-depth network analysis. This Simple Network Management Protocol (SNMP) based network monitoring system lets you detect anomalies instantly. Ensure uptime and fault management of all your SNMP devices with a secure, firewall-friendly architecture.



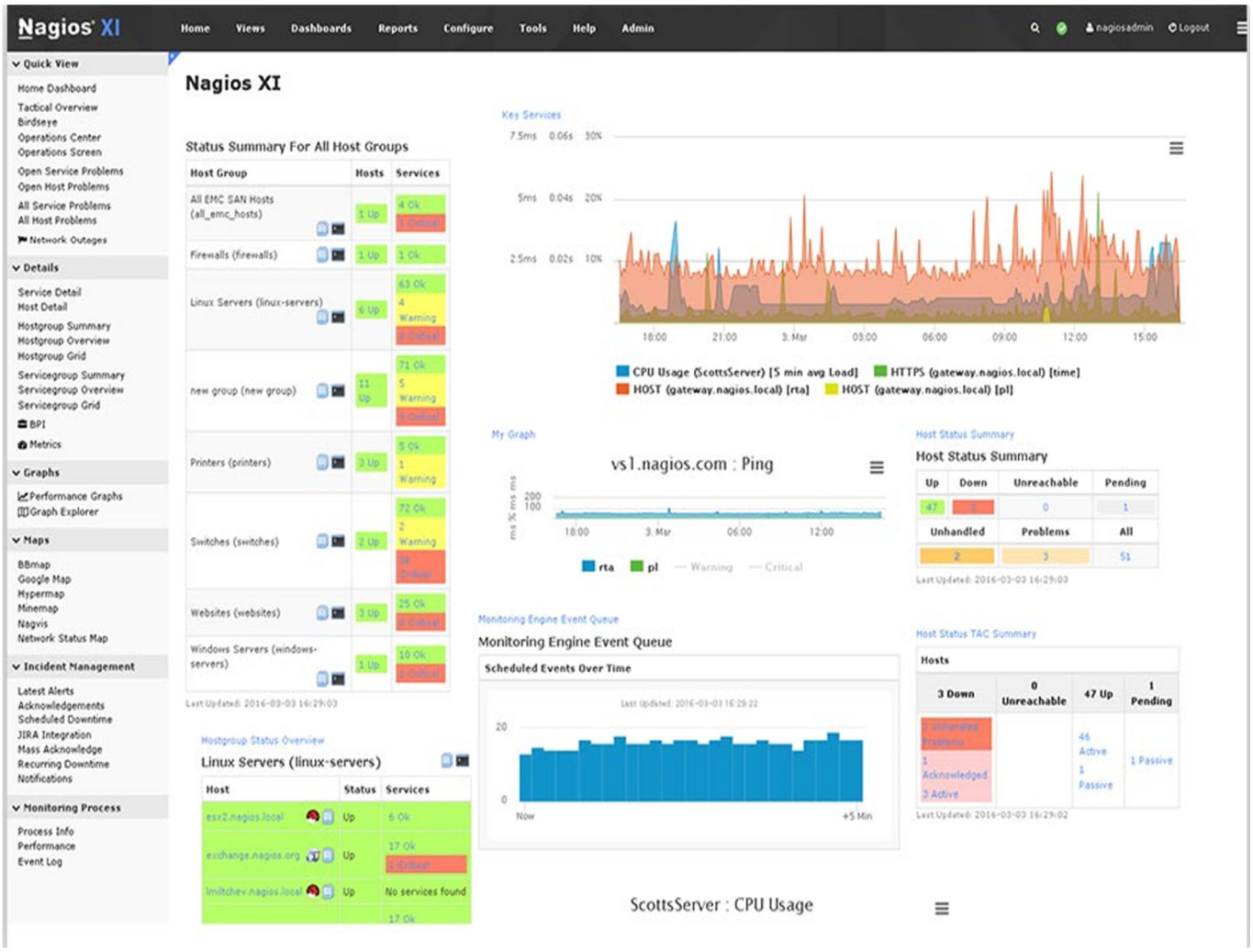
Features:

1) Auto-discovery
2) Multi-vendor Support
3) Device Templates
4) Network Mapping
5) Health Dashboard
6) SNMP Trap Processing
7) Sensor Monitoring
8) Support for Custom MIBs
9) VoIP Monitoring

E. Nagios - The Industry Standard In IT Infrastructure Monitoring

All mission-critical infrastructure components, including as applications, services, operating systems, network protocols, system metrics, and network infrastructure, are monitored by Nagios. Integration with in-house and third-party applications is straightforward thanks to several APIs. Thousands of add-ons created by the community extend the monitoring and native alerting functionality. For monitoring in-house applications, services, and systems, third-party add-ons are available.

According to the company, Nagios is the industry standard for monitoring IT infrastructure. The robust Nagios Core 4 monitoring engine, according to the manufacturer, offers great performance and scalability, as well as high-efficiency worker procedures for monitoring efficacy. Its purpose is to give a company's whole IT operations network and business processes a centralized view. Stakeholders can examine relevant infrastructure status thanks to multi-user access to the web interface. Clients only see the infrastructure components they're authorized for thanks to user-specific views.



Features:

1) Advanced Graphs & Visualizations
2) Performance & Capacity Planning Graphs
3) Configuration Wizards
4) Advanced Infrastructure Management
5) Configuration Snapshot Archive
6) Advanced User Management
7) Service-Level Agreement (SLA) Reports
8) Extendable Architecture

V. RECOMMANDATIONS

The process of selecting a network monitoring solution is unique to your business needs, but the end aim is the same: to provide a consolidated, unified picture of network services activities. Your network administrators should be able to view network operations in detail from a holistic perspective and apply a single strategy for detecting anomalous events.

A. Effective Network Monitoring Delivers

1) Smarter monitoring
2) Enhanced analytics capabilities
3) Faster identification of anomalies
4) Optimized IT operations

B. Before Choosing A Network Monitoring Tools You Should Consider Below Options

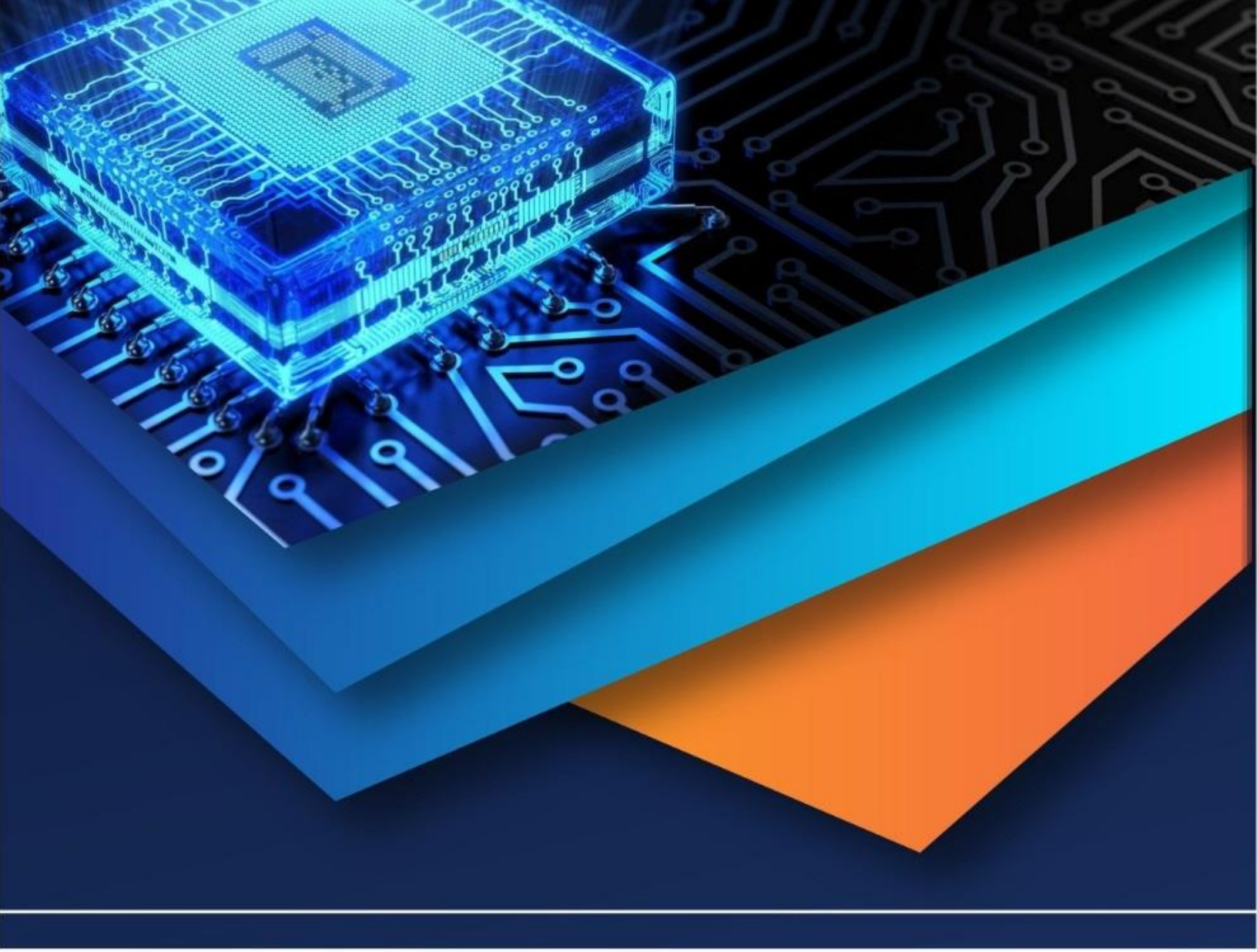
1) Understand Your Preferences
2) Ease of Implementation & Customization
3) Usability
4) Scalability
5) Encryption
6) Automatic Device Discovery
7) Support

VI. CONCLUSSION

Choosing the appropriate network monitoring solution takes time and thought, but having a simple, powerful solution in place may assist increase security and provide better insight into the condition of your network. Furthermore, it can save your company money, time, and worry, allowing you and your staff to concentrate on what matters most: expanding your bottom line.

REFERENCES

[1] https://www.missioncriticalmagazine.com/articles/92664-what-unanticipated-downtime-means-for-your-business
[2] https://www.fema.gov/
[3] https://www.sba.gov/
[4] https://itic-corp.com/blog/2016/08/cost-of-hourly-downtime-soars-81-of-enterprises-say-it-exceeds-300k-on-average/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY